

**AFFIDAVIT IN SUPPORT OF AN APPLICATION
UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE**

STATE OF WEST VIRGINIA
COUNTY OF KANAWHA, to-wit:

I, Terry Hedrick, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. This affidavit is made in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant to search (1) the premises located at 5429 Hillbrook Drive, Cross Lanes, Kanawha County, West Virginia 25313 (the PREMISES), and (2) a black 2004 BMW bearing West Virginia license plate number NNJ878 (the VEHICLE), as more particularly described in Attachment A for the things described in Attachment B.

2. Based on the facts set forth herein, probable cause exists that evidence of violations of 18 U.S.C. §§ 1341 (mail fraud), 1343 (wire fraud), 1349 (conspiracy), 1956-1957 (money laundering), 2314 (transfer of stolen goods), fruits of that criminal activity, and property designed for use, intended for use, or used to commit those offenses are currently located at the PREMISES and in the VEHICLE.

3. I am a Special Agent with the United States Secret Service (hereinafter, the "USSS"), Charleston, West Virginia Resident Office, and have been so employed since December of 2004. I am authorized, pursuant to 18 U.S.C. § 3056(b), to detect and

arrest any person who violates any of the laws of the United States relating to electronic fund transfer frauds, access device frauds, false identification documents or devices, and any fraud or other criminal or unlawful activity in or against any federally insured financial institution. Additionally, I am authorized, pursuant to 18 U.S.C. § 3056(c), to execute warrants issued under the laws of the United States.

4. Since becoming a Secret Service Special Agent, I have personally investigated and/or assisted in investigations relating to violations of the laws of the United States relating to electronic fund transfer frauds, specifically 18 U.S.C. §§ 1028A (aggravated identity theft), 1341 (mail fraud), 1343 (wire fraud), and 1956-1957 (money laundering). I received 30 weeks of training at the Federal Law Enforcement Training Center (FLETC) in Glynco, Georgia and Secret Service's Rowley Training Center in Beltsville, Maryland before my assignment as a Secret Service Special Agent in the Charleston, West Virginia Resident Office. During this training I learned how to investigate violations of the laws of the United States relating to electronic fund transfer frauds, specifically 18 U.S.C. §§ 1028A, 1341, 1343, and 1956-1957.

5. The information contained herein is based on my knowledge, training, and experience, my direct involvement in this investigation, and upon information relayed to me by other law enforcement agents, and other witnesses. Because this Affidavit is

being submitted for the limited purpose of seeking a search warrant for the above-named property, I have not set forth each and every fact learned during the course of this investigation, but simply those facts which I believe are necessary to establish probable cause.

BACKGROUND

6. Since approximately December 2018, the United States Secret Service, the West Virginia State Police, Bureau of Criminal Investigation, the Putnam County Sheriff's Office, and the South Charleston Police Department (SCPD), together with Organized Retail Crimes (ORC) investigators from Kroger, CVS Pharmacy (CVS), and Target Corporation (Target), have been investigating NEDELCHO VLADIMIROV (hereinafter "VLADIMIROV") for violations of 18 U.S.C. §§ 1341 (mail fraud), 1343 (wire fraud), 1349 (conspiracy), 1956-1957 (money laundering), and 2314 (transfer of stolen goods). These violations arise from VLADIMIROV's operation of a fraudulent scheme involving the interstate shipment of stolen goods.

7. As part of the scheme, VLADIMIROV has enlisted a crew of "boosters" who steal the merchandise from local retail stores and sell the stolen merchandise to VLADIMIROV, who then sells the stolen merchandise online marketplaces such as eBay at a higher price. Boosters usually have very specific items in mind when perpetrating their schemes; usually driven at the direction of a fencing

operation. Heavily targeted items tend to be those that are in high demand and of a high value relative to their size, ease of theft and profitability on the secondary market. Many of the known boosters are drug users addicted to controlled substances, who use the money received from VLADMIROV to support their drug habits.

BACKGROUND: ORIGIN OF INVESTIGATION

8. In November 2018, a CVS store in Hurricane, West Virginia, was impacted by a booster targeting Prevagen memory pills, which is an item commonly stolen and re-sold in fencing operations. Based on this information, a notice advising law enforcement and retail partners in the local area to "be on the lookout" (BOLO) for the subject was issued. Target Market Investigator Nicholas Niehaus (MI Niehaus) later contacted CVS Pharmacy ORC Manager Jose Varela and stated the same subject booster from the BOLO had also impacted Target stores in the Southern District of West Virginia area for several months.

9. From on or about September 10, 2018 to on or about December 29, 2018, known boosters Jonathan Marcus (hereinafter "Marcus") and Steven Anderson (hereinafter "Anderson") impacted South Charleston and Barboursville Target stores on multiple occasions for an estimated loss to Target of \$1,500. Target Asset Protection ultimately identified the booster through an apprehension of Steven Anderson. Anderson was known to travel with

Jonathan Marcus, who had also been identified through an apprehension.

10. During the booster interview, Marcus indicated to MI Niehaus that the two men would take the stolen merchandise to a local fencer known only as "Ned," who was later identified as NEDELTCCHO VLADIMIROV. Based on information developed in the interview with Marcus and by investigators subsequent to the interview, it is believed that VLADIMIROV has 15-20 drug users "boosting" for him. VLADIMIROV communicates with boosters by phone or electronic messaging service to provide lists of targeted items to the boosters. Following a theft, VLADIMIROV typically meets the booster at the Speedway convenience store and gas station located at 5296 Big Tyler Road, Charleston, West Virginia, which is 1.5 miles from the VLADIMIROV's residence. VLADIMIROV pays boosters anywhere from 10%-40% of the retail value of the stolen item.

11. In January 2019, MI Niehaus and ORC Manager Varela met with detectives with the SCPD. MI Niehaus and ORC Manager Varela provided detectives with the SCPD with the factual background of their investigation to that point, and the SCPD began their own investigation into prior retail theft arrests in their jurisdiction. The SCPD determined that numerous arrest interviews were consistent and implicated VLADIMIROV as the suspected fencing operator in the South Charleston area.

BACKGROUND: BOOSTER APPREHENSIONS

12. On December 29, 2018, Marcus was apprehended at the South Charleston Target store for theft of two Nest Cameras valued at \$338.00. During the post-apprehension interview, Marcus indicated he was stealing the item to sell to VLADIMIROV, who buys stolen product from multiple subjects to resell online.

13. On September 11, 2019, Stephanie Miller (hereinafter "Miller") was apprehended at South Charleston, West Virginia, Target store for theft of a purse. During the interview, Miller indicated she steals items from area retail stores to sell to VLADIMIROV. Miller stated multiple subjects, herself included are sent lists from VLADIMIROV. Miller steals and sells the items to VLADIMIROV to support their drug habits.

BACKGROUND: SURVEILLANCE

14. Based on information received from retail investigators conducting interviews on theft subjects from Target located at 30 RHL Blvd South Charleston, West Virginia, investigators conducted surveillance on VLADIMIROV on three separate occasions: February 19-21, 2019, May 21-24, 2019, and October 22-24, 2019. Investigators observed VLADIMIROV shipping multiple packages a day at the post office located at the intersection of Doc Bailey and Big Tyler Rd in Cross Lanes, West Virginia, as well as the FedEx location in Cross Lanes, West Virginia.

15. VLADIMIROV was observed on three occasions by Target, CVS, and SCPD investigators meeting subjects to purchase items in his Black BMW bearing West Virginia License Plate NNJ878. On almost every occasion, VLADIMIROV would travel to the U.S. Post Office located at 5306 Big Tyler Road, Charleston, West Virginia, in the early to mid-afternoon time. VLADIMIROV was seen meeting with known boosters and conducting transactions in public parking lots in Cross Lanes and Teas Valley, West Virginia. Detectives and Retail investigators have observed VLADIMIROV conduct multiple meetings with subjects known for theft activity in the Charleston, West Virginia area. VLADIMIROV conducts these transactions from inside his black 2004 BMW.

16. On October 23, 2019, surveillance was conducted of VLADIMIROV at the U.S. Post Office located at 5306 Big Tyler Road, Charleston, West Virginia. At 2:39 p.m., VLADIMIROV arrived at the post office in his black 2004 BMW bearing West Virginia license plate number NNJ878. VLADIMIROV entered the Post Office with several packages. At 2:41 p.m., VLADIMIROV exited the Post Office, returned to his vehicle, and left the property. Mobile surveillance was established at that time. At 2:57 p.m., VLADIMIROV arrived at the McDonald's restaurant located at 4175 WV-34, Hurricane, West Virginia. At 2:59 p.m., VLADIMIROV remained in the black 2004 BMW, and a white female with a yellow sweatshirt and black backpack was observed on foot walking from behind the

McDonald's approached and then entered the passenger side of the vehicle.

BACKGROUND: EBAY SALES

17. After validating information received from theft suspects and confidential informants provided by the SCPD and Putnam County Sheriff's Office, investigators contacted the eBay Investigations Unit in an attempt to identify the eBay account being used by VLADIMIROV. Investigators provided eBay with known identifiers of VLADIMIROV and were able to identify an active eBay account under his control: nedined. Based on these findings, investigators requested all transaction/sales data for the account from October 30, 2017 to October 29, 2019.

18. Review of the items being sold by VLADIMIROV on eBay include a multitude of categories: vitamins, over-the-counter medications, personal care items, electronics, pet-related items, tools, kitchen products, toys, RING doorbell systems, and home care items, among others.

19. From October 30, 2017 to October 29, 2019, 3,676 items were sold on eBay by VLADIMIROV to buyers throughout both the United States and internationally. \$369,818.62 in merchandise was sold by VLADIMIROV during this timeframe.

20. Most recently, an updated request for information was completed for eBay listing data from January 22, 2019 to January 22, 2020. In that time, VLADIMIROV listed and sold 1,761

items. During that time frame, VLADIMIROV's eBay sales totaled \$200,897.23.

21. Investigators have analyzed VLADIMIROV'S eBay account and were able to correlate reports of stolen items with items listed on VLADIMIROV's eBay account within days of theft offenses. Utilizing shortage inventory counts, items missing from Target, CVS, and Kroger stores were identified as being listed for sale or already sold on VLADIMIROV's account.

22. Investigators have continued to monitor known theft reports and can correlate theft incidents by subjects known to sell to VLADIMIROV with exact items being listed on VLADIMIROV's eBay account.

23. As of January 23, 2020, VLADIMIROV has over 3,404 items listed for sale on his eBay account.

BACKGROUND: FINANCIAL INVESTIGATION

24. VLADIMIROV's bank accounts at City National Bank for the period December 2017 to November 2019 were analyzed, and the following information was derived:

(a) Account # XXX8889 - VLADIMIROV deposited numerous Postal money order, pay pal transfers, raise.com transfers (Raise.com is an e-commerce platform owned and operated by Raise that enables third-party sellers to sell new or used Gift Cards on a fixed-price online marketplace alongside Raise's regular offerings), and currency; VLADIMIROV withdraws a lot of money in currency out of this account, as evidenced by him taking out over \$76,000 from ATM withdrawals. Investigators believe this is some of the currency he used to pay for stolen goods from the boosters.

(b) A majority of the deposits into this account are from PayPal. PayPal is the avenue that processes payments when merchandise is bought and sold on EBay. These PayPal deposits totaled over \$263,000.00.

(c) VLADIMIROV transferred over \$250,000 from this City National Bank account to his savings account at City National Bank (Account# 9110074623).

(d) Total Deposits to VLADIMIROV'S Acct XXX8889 at City National Bank totaled over \$420,000.00.

(e) Over \$272,000 was transferred to VLADIMIROV's Savings account at City National Bank (\$155,000 was later transferred back to VLADIMIROV'S acct # 8889 at City National Bank, and he then wrote a check to transfer \$150,000 to his account at JP Morgan Chase Bank).

BACKGROUND: CONTROLLED SALES

25. On January 23, 2020, Confidential Informant 18-8400-009 (CI), also known as "John," made a controlled phone call to VLADIMIROV. The CI told VLADIMIROV that he had two Phillips Norelco electric razors from Target, and a meeting was set up at the Speedway parking lot at 5296 Big Tyler Rd, Charleston, West Virginia. TFO K.A. Davis with the Violent Crime and Drug Task Force West drove the CI to the meeting location. VLADIMIROV arrived on scene in his black 2004 BMW, and the CI got into the passenger side of the vehicle with him. VLADIMIROV looked at the items and paid the CI \$40. The CI then exited the vehicle, reentered the undercover vehicle with TFO Davis. The CI delivered the U.S. currency to TFO Davis and was debriefed.

26. On January 28, 2020, TFO Davis, acting in an undercover capacity, made a controlled phone call to VLADIMIROV. TFO Davis claimed to be friends with "John" and told VLADIMIROV that he had a RING doorbell. VLADIMIROV agreed to meet TFO Davis at the Speedway parking lot at 5296 Big Tyler Rd, Charleston, West Virginia. VLADIMIROV arrived on scene in his black 2004 BMW, and TFO Davis entered the vehicle with him. TFO Davis produced the stolen Ring door bell system and stated, "I don't know how much I get can get for this." VLADIMIROV then used his mobile electronic device to look up the item on eBay and told TFO Davis he could pay him \$35. TFO Davis agreed. TFO Davis then told VLADIMIROV that he wanted to make more money and asked what items VLADIMIROV wanted. VLADIMIROV stated that the more expensive the item the more TFO Davis would get paid. VLADIMIROV indicated that he was looking for Apple products like iPad Pro's.

27. On January 29, 2020, TFO Davis, acting in an undercover capacity, made a controlled phone call to VLADIMIROV. TFO Davis told VLADIMIROV that he had some more items to sell. VLADIMIROV agreed to meet TFO Davis at the Speedway parking lot at 5296 Big Tyler Rd, Charleston, West Virginia. VLADIMIROV arrived on scene in his black 2004 BMW, and TFO Davis entered the vehicle with him. TFO Davis produced the stolen tooth brushes and stated "I got these from CVS and the tag on the shelf said they were

\$150.00." VLADIMIROV then became very suspicious and asked to see TFO Davis's phone. VLADIMIROV asked what kind of phone it was, and TFO Davis responded that he did not know because it was a phone his mom gave him and it is on her plan. VLADIMIROV then asked to see the phone. TFO Davis handed VLADIMIROV the phone. VLADIMIROV then inspected it by examining the call history and text messages as well as cycling through the applications. VLADIMIROV then closed all of the applications running on the phone, which cancelled the covert recording application that was recording the controlled sale. VLADIMIROV then told TFO Davis that he did not know if he wanted the electric toothbrushes because he sells all the merchandise on eBay, and other eBay listings had the item listed at \$35.00. After some deliberation, VLADIMIROV decided that he could give TFO Davis \$30 for the electric tooth brushes. TFO Davis then stated that he would call VLADIMIROV again tomorrow, and VLADIMIROV agreed that would be fine. No audio or video of this controlled sale was obtained due to technical difficulties.

BACKGROUND: ITEMS TO BE SEIZED

28. Based upon my experience and training, consultation with other law enforcement officers experienced in fraudulent schemes, and all facts and opinions set forth in this affidavit, I know that:

1. Individuals conducting fraudulent schemes involving the interstate shipment of stolen goods often maintain in their residences an inventory of stolen items.

2. Individuals conducting fraudulent schemes often rely on others to obtain their inventory. Frequently, such individuals maintain evidence of the identities of these co-conspirators at their residence and on their mobile electronic devices.

3. Individuals conducting fraudulent schemes involving the interstate shipment of stolen goods commonly use cash to facilitate the scheme. In order to do this, such individuals frequently attempt to secrete, transfer and conceal the money by means, including, but not limited to: placing assets in the names other than their own to avoid detection while maintaining control; laundering the money through what appears to be legitimate business or businesses; hiding money in their homes, safes and safety deposit boxes; or using the money to buy assets which are difficult to trace. Records of these and other types of transactions are often found at residences and on the mobile electronic devices of individuals involved in the fraudulent schemes.

4. Residences and premises used by individuals conducting fraudulent schemes contain articles of personal property evidencing the identity of person(s) occupying, possessing,

residing in, owing, frequenting or controlling the residence and premises.

5. Individuals conducting fraudulent schemes involving the interstate shipment of stolen goods frequently communicate with co-conspirators by means of mobile electronic devices and usually maintain these items on their person and/or in their residences and vehicles.

6. Individuals conducting fraudulent schemes involving the interstate shipment of stolen goods often maintain photographs, and/or audio and video recordings of their associates or personal property which were acquired with proceeds or property utilized to facilitate the scheme. Such items are typically maintained in their residences and on mobile electronic devices. Such individuals often store information relating to their illegal business on computers and/or computer disks.

7. It is also my opinion and belief that the above-described documents are currently possessed by individuals maintaining an illegal business much the same way a legitimate business will maintain records and tools of its trade whether or not the business has a particular item in inventory on a given date. These documents are kept by illegal businesses whether or not the illegal business is in possession of any stolen goods at any given moment. I believe that the seizure of such documents will provide evidence of the events set forth in this affidavit

and that such documents can be found at the target location despite any lapse of the time between the events described and the anticipated search pursuant to this warrant.

8. The investigation into the criminal activities of VLADIMIROV reveals that fraudulent schemes involving the interstate shipment of stolen goods is ongoing. Due to the quantity of stolen goods being moved and the relatively sophisticated manner in which VLADIMIROV conducts his illegal activities, I believe he has been engaged in the illegal scheme for a long period of time. As a consequence, I believe that the items described in Attachment B will provide evidence of the events set forth in this affidavit and that such articles can be found at the PREMISES and in the VEHICLE, despite any lapse of time between the events described and the anticipated search pursuant to this warrant. I further believe that items and articles described in Attachment B can be located in any garage, vehicle, or outbuilding on the PREMISES.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

9. As described above and in Attachment B, this application seeks permission to search for records that might be found on the PREMISES, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially,

the copying of electronically stored information, all under Rule 41(e) (2) (B).

10. *Probable cause.* I submit that if a computer or storage medium is found on the PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating

system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

11. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this

forensic electronic evidence will be on any storage medium in the PREMISES because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.
- b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation,

thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculcating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such

information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt

(e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

- c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes

it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

12. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

- a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable.

As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

13. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

PROBABLE CAUSE TO SEARCH THE RESIDENCE OF NEDELTCO VLADIMIROV

14. The PREMISES to be searched is the residence of NEDELTCO VLADIMIROV, and is located at 5429 Hillbrook Drive, Cross Lanes, Kanawha County, West Virginia 25313, and within the Southern District of West Virginia.

15. According to the Kanawha County Clerk's Office records, Deed Book 2813 Pages 245 - 249, this property (2 lots) was purchased by NEDELTCO VLADIMIROV and Desislava D. Vladimirov on March 2, 2012 for \$168,892.00. It is believed that VLADIMIROV is divorced and lives at the residence alone.

16. Information obtained to date reflects VLADIMIROV does not have legitimate employment. West Virginia Secretary of State records reflect that VLADIMIROV was the President and Incorporator of Transglobal Enterprises Inc. using his residence in Cross Lanes

as the place of business, effective February 1, 2013. However, the company was dissolved by VLADIMIROV, effective October 23, 2013.

17. Based on information developed in the investigation and summarized more fully above, I have probable cause to believe that VLADIMIROV has operated an unlicensed business out of his residence in Cross Lanes, West Virginia, and within in the Southern District of West Virginia, since October 2017 to the present. VLADIMIROV purchases merchandise stolen from local businesses from associates known as boosters and enlisted by VLADIMIROV to steal the items. VLADIMIROV transports the stolen items to his home in Cross Lanes and lists the items for sale on eBay. Upon the sale of the item, VLADIMIROV packages the item and brings packages to shipping services, such as the U.S. Postal Service, UPS, and FedEx. VLADIMIROV then transferred the proceeds from the sales to bank accounts to further promote the operations of his unlicensed business, as well as to conceal and disguise the source, origin, nature, ownership, and control of the proceeds. Some of the transfers were greater than \$10,000.

18. An interview of a confidential informant (Steven White) signed on with Putnam County Sheriff's Office was conducted on October 30, 2019, at the Putnam County Detective Bureau office by TFO Sgt. Deskins, Target Investigator Nicholas Niehaus, and CVS Investigator Jose Varela. During the interview, White stated VLADIMIROV purchased items from at least fifteen subjects White

was associated with during the last three years. White stated he and others have been in VLADIMIROV's residence, and it is known that stolen product is stored in both VLADIMIROV's basement and garage structure next to the house. White stated it was set up on shelves. White provided investigators more than ten names that White had known personally or been in a vehicle with VLADIMIROV during a sale of stolen product to VLADIMIROV. White stated VLADIMIROV would meet at Speedway located at 5296 Big Tyler Road, Charleston, West Virginia. VLADIMIROV would travel to Teays Valley to meet to purchase product, but would provide the boosters of stolen product a much lower rate if VLADIMIROV had to travel a longer distance to make the transaction.

PROBABLE CAUSE TO SEARCH THE VEHICLE OF NEDELTCO VLADIMIROV

19. The VEHICLE to be searched is the black 2004 BMW bearing license plate number NNJ878 is titled in the name of NEDELTCO VLADIMIROV and Desislava D. Vladimirov. It is believed that VLADIMIROV is divorced, and the VEHICLE is used exclusively by VLADIMIROV.

20. Investigators and detectives have observed VLADIMIROV driving the black 2004 BMW to meet with the boosters. VLADIMIROV uses this vehicle to deliver packages containing the stolen merchandise to the U.S. Post Office, FedEx and to UPS. According to post-apprehension and arrest statements, subjects will enter the passenger side of his vehicle and conduct a cash transaction

inside the vehicle. During controlled purchases, items to facilitate the scheme, including significant amounts of cash, have been observed inside of the vehicle.

CONCLUSION

21. I submit that this affidavit supports probable cause for a warrant to search the PREMISES and VEHICLE described in Attachment A and seize the items described in Attachment B.

Further your affiant sayeth naught.



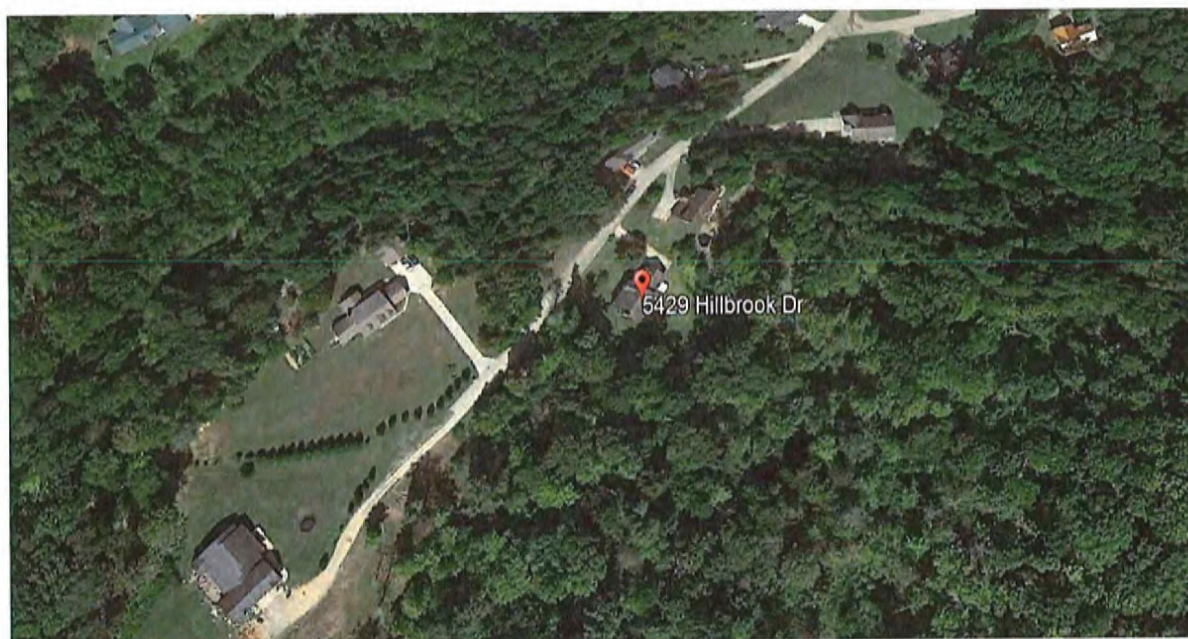
SPECIAL AGENT TERRY HEDRICK,
UNITED STATES SECRET SERVICE

Sworn to before me, and subscribed in my presence, this ____
Day of January, 2020.

THE HONORABLE DWANE L. TINSLEY
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

(1) The residence, all structures, vehicles, and curtilage located at 5429 Hillbrook Drive, Cross Lanes, Kanawha County, West Virginia 25313. A two (2) story frame structure with an attached garage and off-white vinyl siding used as a single family home. There are two covered porches on the right side of the structure, one on each level with a front entrance door which is concealed to the right of the front bay windows that protrude from the front of the house. The rear of the house has a small wooden deck that has railing and a gate. There is also an out building that is backed against the house immediately adjacent to the garage side of the residence. This structure is a primary residence and also known to be used to store and maintain products obtained and warehoused for an online business. There is one known occupant residing in this structure full time. A young adult child may stay at the residence on some weekends, holidays and summers. The coordinates for this structure is the approximate latitude of 38.4442590, and the approximate longitude of -81.7754690.





Kanawha County Assessor			
Summary			
Parcel ID (Account)	25 16R005700000000	Legal Description 2	SUB HILLBROOK DR 5429
Tax Year	2018	Legal Description 3	
Neighborhood	604K	Year Built	1998
District	25 Union	Total Rooms	7
Map	16R	Bed Rooms	4
Parcel	57	Full Baths	2
Sub Parcel		Half Baths	1
Special Id		Additional Fixtures	4
Tax Class	Class 2	Total Fixtures	12
Land Use	101 Residential 1 Family	Heating	Central A/C
Calculated Acres	0.33	Heating Fuel Type	Electricity
Property Class	Residential	Living Area (SF)	2030
Assessed Land	\$ 11,640.00	State	WV
Assessed Building	\$ 84,180.00	City	CROSS LANES
Mineral Value	\$ 0.00	Zip Code	26313
Homestead Value	\$ 0.00	Count	1
Total Assessed Value	\$ 95,820.00	Pricing Method	F
Owner's Name	VLADIMIROV DE SISLAVA D &	Total Acres	0.33
Owner's Mail Address	5429 HILLBROOK DR	Land Price	\$ 19,420.00
Owner's Mail Address		Last Sale Price	\$ 18,000.00
Location	5429 Hillbrook Dr	Last Sale Apr	
Deed Book	2813	Sales Ratio	
Location	5429 HILLBROOK DR	Sale Year	1998
Page	0245	Last Sale Date	08/01/1998
Homestead		Price per Sqft	\$ 9.31
Street Name	HILLBROOK	Sales Ratio	5.07
Legal Description 1	LT 3 SEC 7 BROOKSIDE VILLAGE	Appraisal per Sqft	\$ 47.20

[< Search Results] [Show All Fields]

- (2) A black 2004 BMW 4-door sedan bearing West Virginia license plate number NNJ878. The vehicle is labeled as a model 330xi with black tinted windows. The lower left hand corner of the back windshield has an oval sticker that is white, green and red surrounding the letters "BG." There are two grey fixtures protruding from the truck deck lid that appear to be a broken spoiler, the left one is higher than the right one. There is a rear license plate frame that is black with the letters BMW centered in black surrounded by white contrast at the bottom.



ATTACHMENT B

1. All records relating to violations of 18 U.S.C. §§ 1341 (mail fraud), 1343 (wire fraud), 1349 (conspiracy), 1956-1957 (money laundering), and 2314 (transfer of stolen goods), those violations involving NEDELTCCHO VLADIMIROV and occurring after October 30, 2017, including:

- a. retail items, including but not limited to, vitamins, over-the-counter medications, personal care items, electronics, pet-related items, tools, kitchen products, toys, RING doorbell systems, and home care items;
- b. records and information relating to the interstate shipment of stolen goods, including but not limited to, ledgers, receipts, financial documents, bank statements, lists of telephone numbers or other contact information, identifying information of customers and/or suppliers of stolen goods;
- c. evidence of occupancy: utility bills, deeds, mortgage records, identification documents, and mail; and
- d. fruits of criminal activity: U.S. currency, all documents showing the purchase, ownership, lease (as lessor or lessee), or sale of any asset, personal or real to include automobiles, boats, motorcycles or similar motorized conveyances to include deeds, titles, and bills of sale.

2. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

- a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
- b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- c. evidence of the lack of such malicious software;
- d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;
- e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;

- f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
- g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
- h. evidence of the times the COMPUTER was used;
- i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
- j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
- k. records of or information about Internet Protocol addresses used by the COMPUTER;
- l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;
- m. contextual information necessary to understand the evidence described in this attachment.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer

or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

inside the vehicle. During controlled purchases, items to facilitate the scheme, including significant amounts of cash, have been observed inside of the vehicle.

CONCLUSION

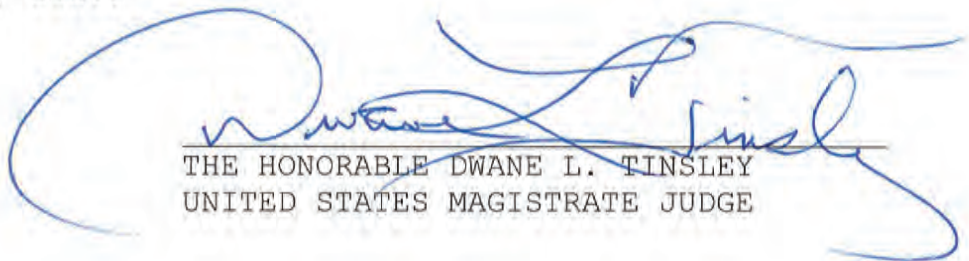
21. I submit that this affidavit supports probable cause for a warrant to search the PREMISES and VEHICLE described in Attachment A and seize the items described in Attachment B.

Further your affiant sayeth naught.



SPECIAL AGENT TERRY HEDRICK,
UNITED STATES SECRET SERVICE

Sworn to before me, and subscribed in my presence, this 3rd
Day of February, 2020.



THE HONORABLE DWANE L. TINSLEY
UNITED STATES MAGISTRATE JUDGE